11-06-00

A

Please type a plus sign (+) inside this box → +

PTO/SB/05 (08-00)
Approved for use through 10/31/2002. OMB 0651-0032
U S Patent and Trademark Office: U S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	042390.P10142
First Inventor	Oleg Rashkovskiy
Title	CONTENT PROTECTION USING BLOCK REORDERING
Express Mail Label No.	EL034435845US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)

2. ☐ Applicant claims small entity status.
See 37 CFR 1.27.

3. ☒ Specification [Total Pages 22]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to sequence listing, a table, or a computer program listing appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

4. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 5]

5. Oath or Declaration [Total Pages 6]
a. ☐ Newly executed (original or copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 17 completed)
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b)

6. ☐ Application Data Sheet. See 37 CFR 1.76

7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)

8. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Form (CRF)
b. Specification Sequence Listing on:
i. ☐ CD-ROM or CD-R (2 copies); or
ii. ☐ paper
c. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s))
10. ☐ 37 C.F.R. § 3.73(b) Statement (when there is an assignee) ☒ Power of Attorney
11. ☐ English Translation Document (if applicable)
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☒ Other: CHECK FOR $2,478.00

17. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____
Prior application Information: Examiner _____ Group/Art Unit: _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

18. CORRESPONDENCE ADDRESS

☒ Customer Number or Bar Code Label 08791
PATENT TRADEMARK OFFICE
(Insert Customer No. or Attach bar code label here)

or ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Fax	

Name (Print/Type)	Paul A. Mendonsa	Registration No. (Attorney/Agent)	42,879
Signature	Paul A. Mendonsa	Date	11/02/00

Burden Hour Statement This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U S Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

PTO/SB/17 (08-00)
Approved for use through 10/31/2002. OMB 0651-0032
U S Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 2,478.00

Complete if Known	
Application Number	
Filing Date	November 2, 2000
First Named Inventor	Oleg Rashkovskiy
Examiner Name	
Group/Art Unit	
Attorney Docket No.	042390.P10142

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

☐ Charge Any Additional Fee(s) Required Under 37 CFR §§ 1.16, 1.17, 1 18 and 1.20.

☐ Applicant claims small entity status. See 37 CFR 1.27.

2. ☒ **Payment Enclosed:**

☒ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710.00
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 710.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		
Total Claims	96	- 20** =	76	X	18.00	=	$1,368.00
Independent Claims	8	- 3** =	5	X	80.00	=	$400.00
Multiple Dependent						=	

**or number previously paid, if greater, For Reissues, see below

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	260	204	135	Multiple Dependent claim, if not paid
109	80	209	40	**Reissue independent claims over original patent
110	18	210	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 1,768.00

FEE CALCULATION (continued)

3. ADDITIONAL FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	*Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	*Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	390	216	195	Extension for response within second month	
117	890	217	445	Extension for response within third month	
118	1,390	218	695	Extension for response within fourth month	
128	1,890	228	945	Extension for response within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	126	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($)

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Paul A. Mendonsa	Registration No. (Attorney/Agent)	42,879	Telephone	(503) 684-6200
Signature	Paul A. Mendonsa			Date	11/02/00

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2039.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

UNITED STATES PATENT APPLICATION

Title:

CONTENT PROTECTION USING BLOCK REORDERING

Inventors:

Oleg Rashkovskiy

Eric C. Hannah

Docket No.: 42390.P10142

Prepared by:
Richard C. Calderwood
Reg. No. 35,468

Express Mail No.: EL034435845US

CONTENT PROTECTION USING BLOCK REORDERING

Background of the Invention

Technical Field of the Invention:

The present invention relates generally to data security, and more specifically to a technique for protecting digital content by reordering blocks of a data set.

Background Art:

Various types of data are transmitted or otherwise transferred from one entity, such as a server, to another entity, such as a client computer or a television set-top box, via various communication paths such as broadcast, wireless, cable, modem, LAN, DSL, CD-ROM "sneakernet", and so forth. The content of such data transmissions may be, for example, digital video, digital audio, database, graphics, spreadsheet, text, or any other form of content. The content may contain a movie, a song, a book, a television show, an electronic programming guide (EPG), an advertisement, advanced television enhancement information (ATVEF), a digital gift certificate, a digital coupon, an executable file, a data file, or any other content whatsoever. When this patent discusses examples such as a cable television company server sending an EPG to a subscriber's set-top box, the reader will understand that the invention is not necessarily limited to the specific example given, but rather that the example is given to help the reader understand the invention.

Content providers may desire to prevent corruption and/or piracy of their content, not only during transmission but also thereafter during such time as the content is stored at the receiving entity. One mechanism commonly employed to protect content is encryption, in which the digital values within the content are altered according to a cipher prior to their transmission. Many encryption schemes and methodologies are well known in the art, and will not be discussed in detail in this patent. It is assumed that the skilled reader is familiar with the relevant art.

It is also well understood that encryption of a large data set, such as a full-length movie, requires a relatively large amount of computational power and time, and that not all applications lend themselves to expense of power and/or time. This may be especially true of content which has limited economic value or which has a sufficiently short useful lifetime. The lower the value of the content, and the shorter its useful lifetime, the less justification there may be for using expensive encryption technologies to protect that content.

It is also understood that there may be many avenues of attack against content protection, with different levels of risk. Content may be attacked by different sets of actors using different sets of tools. In general, the easier and less expensive the attack, the larger the set of people who will be engaged in it. For some types of content, it may not be necessary – economically or otherwise – to protect content against all types of attack by all classes of people. For example, while the owner of a major motion picture may deem it necessary to provide strong encryption on every byte of the content at all stages of transmission and storage, the owner of an electronic programming guide covering only the next few days' broadcasts may deem it sufficient to use a weaker (and less costly) protection mechanism.

Some content, such as perhaps a nation's military secrets, may be so valuable that, in the example of a computer, it is not only desirable to protect the content which is stored on the hard drive, but further to prevent snooping attacks directed against internal wires, electromagnetic emanations from the keyboard and CRT, and so forth, on occasion even including the use of self-detonating chips which destroy themselves and their contents if someone attempts to break them open to peer inside with an electron microscope. On the other end of the spectrum, some content may be adequately protected if it is simply protected against software attacks such as those done via debuggers or memory dumps.

Brief Description of the Drawings

The invention will be understood more fully from the detailed description given below and from the accompanying drawings of embodiments of the invention which, however, should not be taken to limit the invention to the specific embodiments described, but are for explanation and understanding only.

FIG. 1 shows one embodiment of a system which employs this invention, including a server and a client.

FIG. 2A shows how content is stored according to the prior art.

FIG. 2B shows how one type of file system operates according to the prior art, such as may be used in a system which operates as shown in FIG. 2A.

FIG. 3A shows how content is stored according to one embodiment of this invention, in which blocks of respective files are reordered within the separate storage areas allocated to such files.

FIG. 3B shows how a file system may operate according to the embodiment of this invention illustrated in FIG. 3A.

FIG. 3C shows a data handle table which may be utilized by another embodiment of a file system which operates according to the principles of FIG. 3A.

FIG. 4A shows how content is stored according to another embodiment of this invention, in which blocks of files are reordered within the overall storage space.

FIG. 4B shows how a file system may operate according to the embodiment illustrated in FIG. 4A.

FIG. 4C shows a data handle table for a file system which operates as illustrated in FIG. 4A.

FIG. 5 illustrates a recordable medium having disposed thereon one or more reordered content items.

Detailed Description

FIG. 1 shows a system 50 including a Server in communication with a Client. As mentioned above, these are only illustrative examples, and the invention is not limited to server/client applications.

The Server contains or has access to some Original Content which is desired to protect against attack. Rather than transmit the Original Content in its unsecured form to the Client (because the Original Content could be intercepted along its transmission path), the Server performs operations upon the Original Content to create Reordered Content. This may optionally be done in conjunction with conventional encryption, but it is not necessary.

In these operations performed by the Server, blocks of the Original Content are rearranged according to an algorithm. In one embodiment, the algorithm employs a random number generator (not shown) to select reordered positions for blocks. In one embodiment, it may further select a block size using the random number generator. A predetermined reordering pattern could be employed, but a more non-deterministic scheme may offer greater security.

In some applications, the reordering scheme may be employed to permit a single, specified client to utilize the transmitted content, while blocking access by all others – for example, a cable operator may wish to permit only a specified, individual, fee-paying client to view a particular pay-per-view movie (or rather, a particular reordered version thereof). In other applications, the reordering scheme may be employed to permit a multitude of clients to utilize the transmitted content

while preventing others from utilizing it – for example, in a cable television system in which a common coaxial cable network is shared by a plurality of cable television operators, each operator may wish to permit any and all of its own subscribers to view a particular movie, while preventing the other cable operators' subscribers from viewing it.

The blocks which are being rearranged may be the same size, or they may vary in size. Same size lends itself to simpler processing, while varying size may lend itself to improved security.

In FIG. 1, the Client is shown as containing a Client ID. This could be a unique identifier such as a serial number, or it could be a possibly-unique identifier such as a random prime number or the like. Alternatively, the Client ID could be unique to a group (such as all cable boxes provided by this cable operator, or all cable boxes provided by this cable operator to purchasers of a certain subscription level).

In some embodiments, the Server may contain a copy of each Client's Client ID. For example, the Server can simply keep a list of Client IDs as new Clients are provisioned by the Server; alternatively, the Client could communicate its Client ID to the Server under a public-key encrypted and certificate-verified dialog. The Client ID could be a permanent feature of the individual Client, or it could be e.g. a session key generated by the client and securely communicated to the Server by known data security means.

Once the Server is in possession of the Client ID, it uses a Key Generator to produce a reordering Key. A Reorderer takes as input the Original Content, and, in a manner dictated by the reordering Key, generates the Reordered Content. Different Clients may have different Client IDs, with the result that for the same Original Content, their respective Reordered Content may well be in different orders and neither Client will be able to restore the Original Content from the other's Reordered Content.

The Server may include a Transmitter which sends the Reordered Content to the Client over a Reordered Content Channel of a communication medium. The Transmitter may also send the Key to the Client over a Key Channel of the same or a different communication medium. Alternatively, the Reordered Content and/or Key can be written to a storage medium (such as in FIG. 6) and delivered to the Client manually.

The Client contains Storage where the Reordered Content is stored. This may be a hard drive, an optical drive, semiconductor memory, or any other suitable storage means. The Reordered Content may be stored in a read-once manner, or it may be stored in a cache replacement manner

until it is eventually evicted, or it may be stored permanently, or according to whatever storage needs the application dictates.

In one embodiment, the Client contains a Key Generator which generates a Local Key as a function of the Client ID, in a manner corresponding to the generation of the Reordering Key by the Server. The Local Key is the functional inverse of the Reordering Key. In other embodiments, the Local Key can be generated by the Server and transmitted over the Key Channel to the Client; in this case, the Client will not need a Key Generator.

In some embodiments, the Local Key is used repeatedly for all content received from the Server. In other embodiments, each content item, such as each respective movie, may have its own Local Key generated according to the Client ID and some other input such as a timestamp or a value from the content itself. There is no strict requirement that the same reordering key be used for an entire logical content item; in some embodiments, it may be desirable to switch keys one or more times during reordering of a lengthy content item. This may improve security, without unduly increasing system complexity.

The Client further contains a Reorder Structure Generator which utilizes the Local Key to create a Block Reordering Structure, which is in turn used by a Content Retriever to access the Reordered Content according to its original order for use by a Content User. Note that this does not necessarily mean that the Reordered Content must be accessed in linear fashion; the Block Reordering Structure may permit random access, as well. The Content Retriever may be, for example, a hardware disk drive controller. The Content User may be, for example, a software process or task spawned to display the movie.

For improved security, the Client ID, Local Key, and/or Block Reordering Structure may be kept in Protected Memory. In some applications, it may be sufficient that this memory be protected by conventional operating system (OS) schemes whereby one process can be denied access to another process's memory area. In other applications, it may be necessary to take further protective measures, such as by using self-destructive memory devices for the Protected Memory to prevent them being read via means more intrusive than mere software attacks. It may also be necessary to protect busses, wires, and other points of potential physical attack. It may be desirable to prevent physical access such as by burying the protected memory in a layer of plastic. Those technologies are well-known, and may be utilized in practicing this invention, but it is not necessary to discuss their particulars here.

FIG. 2A illustrates how content may be stored in a storage device (generally analogous to the Client's Storage in FIG. 1) according to the prior art. In the example shown, two separate content items are shown stored in the storage – one containing "MOVIE" and one containing "GUIDE". The reader will understand that these content items are not necessarily textual, and that the respective blocks of each do not necessarily contain only a single byte value. These simplistic examples are shown merely for illustrative purposes.

In the storage, there are multiple storage location blocks, generally illustrated by locations 0 to 15 in FIG. 2A. The first content item, "MOVIE", is illustrated as being stored in contiguous locations 2-6. The second content item, "GUIDE", is illustrated as being stored in non-contiguous locations 9-12,15. In many common applications, such as a personal computer, a content item such as a data file is not necessarily stored in contiguous *physical* locations, nor, indeed, in sequential *physical* locations. In such applications, the operating system or other control entity will keep track of where each *logical* block is physically stored. However, even in logically-addressed systems, the contents of a file are stored in linear fashion within that file's allocated storage.

FIG. 2B represents the addressing scheme itself, employed by the operating system. Content item A ("MOVIE") is stored in blocks 2-6, and content item B ("GUIDE") is stored in blocks 9-12,14, which the file system keeps track of via a linked list or other known method.

FIG. 3A illustrates one difference between this invention and the prior art. The same addressing scheme is employed in FIG. 3A as in FIG. 2A. However, the Storage in FIG. 3A contains reordered content: the "MOVIE" content item has been reordered "VIMEO", and the "GUIDE" content item has been reordered "DEUGI". The reordering of the content is orthogonal to the addressing scheme of the storage device.

FIG. 3B shows one embodiment of the Block Reordering Structure (of FIG. 1), in which linked lists are employed, to keep track of the reordered blocks of the stored content items. In accordance with the Client's ID and thus the Local Key (of FIG. 1), the Reorder Structure Generator has generated a structure indicating that the blocks of the content item A ("MOVIE") have been reordered such that the correct order is to retrieve the blocks from blocks 2, 4, 0, 1, and 3 in order; this is, of course, on top of any logical-to-physical addressing scheme employed. If the scheme of FIGS. 3A and 3B is employed, the initial (0^{th}) block of "MOVIE" is found by the Content Retriever accessing the initial (0^{th}) value ("2") from the respective portion ("A") of the Block Reordering Structure, then the operating system or other such entity will use this as an index (loosely speaking)

into the File Structure, and will retrieve the physical location ("4") where that block ("M") is stored in the Storage device. The scheme works that way for any N^{th} block, of course. And it works that way for other content items' retrieval, as well (such as item B, "GUIDE").

FIG. 3C shows an alternative embodiment of a Block Reordering Structure, in which it is a Data Handle Table, rather than a linked list. In the Data Handle Table, which could be a content-addressable memory for example, the locations of the reordered blocks are recorded in what is illustrated as the rightmost column. There needs to be some mechanism of associating these reordered locations with their regularly-ordered counterparts; one suitable option may simply be to record the corresponding values in what is illustrated as the center column. Finally, if the Client is to store more than one reordered content item at a time, there needs to be some mechanism of associating these ordered/reordered value pairs with the content item to which they pertain; one suitable option may be to record an identifier of the respective content item in what is illustrated as the leftmost column. Those skilled in the art will readily appreciate that other embodiments are within their understanding, when armed with this disclosure. For example, the leftmost column could be removed and could be replaced with a functionally similar scheme such as a table which includes one entry per content item, plus an index into the two-column Data Handle Table indicating the first entry for that content item, and that it could further include either an indication of how many sequential entries in the Data Handle Table belong to that content item, or an index to the final entry in the Data Handle Table for that content item. Furthermore, the center column could be removed in some embodiments, and the functionality of its contents could be replaced by logic which indexes into the rightmost column based on the logical block position of a desired block. Finally, it should be understood that if a logical addressing scheme is employed, there will be an OS File System or other such entity performing logical-to-physical address translation to produce Physical Addresses that are used to directly address the Storage medium.

FIG. 4A illustrates an embodiment which does not use logical addressing, and in which the Server has direct control over where in the Client's physically addressed Storage device Reordered Content items are stored. In such a scheme, the values stored in the Block Reordering Structure are physical addresses.

FIG. 4B illustrates how the file system may operate in controlling storage according to the physically-addressed, storage-wide reordering shown in FIG. 4A.

FIG. 4C illustrates an alternative embodiment in which the physical addresses are stored in a Data Handle Table rather than in a linked list. The reader will understand that the functionality of this table may be distributed in a manner similar to that discussed above regarding FIG. 3C.

FIG. 5 illustrates a recordable medium having recorded thereon one or more block-reordered content items. This may be the storage device in the server, wherein is stored a reordered content item prior to or during transmission to a client. Or, it may be the storage device in the client which has received the reordered content item from the server. Or, it may be the transmission medium itself, in the case of a sneakernet delivery mechanism. Or, it could be an archival storage mechanism.

Reference in this specification to "an embodiment," "one embodiment," "some embodiments," or "other embodiments" means that a particular feature, structure, or characteristic described in connection with the embodiments is included in at least some embodiments, but not necessarily all embodiments, of the invention. The various appearances "an embodiment," "one embodiment," or "some embodiments" are not necessarily all referring to the same embodiments.

If the specification states a component, feature, structure, or characteristic "may", "might", or "could" be included, that particular component, feature, structure, or characteristic is not required to be included. If the specification or claim refers to "a" or "an" element, that does not mean there is only one of the element. If the specification or claims refer to "an additional" element, that does not preclude there being more than one of the additional element.

Those skilled in the art having the benefit of this disclosure will appreciate that many other variations from the foregoing description and drawings may be made within the scope of the present invention. Indeed, the invention is not limited to the details described above. Rather, it is the following claims including any amendments thereto that define the scope of the invention.

CLAIMS

What is claimed is:

1. An apparatus comprising:
   a key generator for generating a key according to an identifier value of another apparatus; and
   a reorderer for reordering blocks of an original content item according to the key.

2. The apparatus of claim 1 further comprising:
   a transmitter adapted for distributing the reordered blocks over a wireless broadcast channel.

3. The apparatus of claim 1 further comprising:
   a transmitter adapted for distributing the reordered blocks over a coaxial cable.

4. The apparatus of claim 1 further comprising:
   a transmitter adapted for distributing the reordered blocks over a digital subscriber line (DSL).

5. The apparatus of claim 1 further comprising:
   means for writing the reordered blocks to a removable storage disc.

6. The apparatus of claim 1 further comprising:
   storage means for storing the reordered blocks.

7. The apparatus of claim 1 wherein each of the reordered blocks comprises a same data content as its corresponding block from the original content item.

8. The apparatus of claim 1 wherein the reordered blocks are of a uniform block size.

9. The apparatus of claim 1 wherein the reordered blocks include a first reordered block of a first block size and a second reordered block of a second block size which is different than the first block size.

10. The apparatus of claim 1 further comprising:

means for keeping a list of identifier values of a plurality of such other apparatuses;

wherein, for different identifier values of two such other apparatuses, the key generator generates different keys; and

wherein, in response to the different keys, the reorderer imposes different new block orders on the original content item.

11. The apparatus of claim 10 wherein:

the identifier values in the list are mutually unique; and

the reorderer imposes a unique new block order on the original content item for each such other apparatus.

12. The apparatus of claim 10 wherein:

the list includes a first identifier value for a first such other apparatus, and a second identifier value for both a second and a third such other apparatus, wherein the second identifier value is different than the first identifier value; and

the reorderer imposes a first new block order on the original content item for distribution to the first such other apparatus, and a second, different new block order on the original content item for distribution to either the second or the third such other apparatus.

13. The apparatus of claim 1 wherein the identifier value is a serial number of the other apparatus.

14. The apparatus of claim 1 wherein the identifier value is a random number assigned to the other apparatus.

15. The apparatus of claim 14 wherein the random number has been filtered for primeness and been found to be likely to be prime beyond a predetermined threshold.

16. The apparatus of claim 15 wherein the random number is a prime number.

17. The apparatus of claim 1 wherein:

the apparatus is a server, the other apparatus is one of a plurality of clients, and the server further comprises,

means for provisioning the clients, including the selection of the identifier values for the clients, and

means for maintaining a list of the clients' identifier values.

18. The apparatus of claim 1 wherein the identifier value comprises a session key.

19. The apparatus of claim 1 further comprising:

a transmitter for communicating over a key channel and a content channel.

20. The apparatus of claim 19 wherein the key channel and the content channel are logical channels operating over a same physical medium.

21. The apparatus of claim 1 wherein the original content item comprises an electronic programming guide.

22. The apparatus of claim 1 wherein the original content item comprises ATVEF information.

23. The apparatus of claim 1 wherein the original content item comprises a digital gift certificate.

24. The apparatus of claim 1 wherein the original content item comprises a digital coupon.

25. The apparatus of claim 1 wherein the original content item comprises a movie.

26. The apparatus of claim 1 wherein the original content item comprises an episode of a television show.

27. The apparatus of claim 1 wherein:

the apparatus further comprises a storage device; and

the reorderer reorders blocks of the original content item and stores them to the storage device according to a logical addressing system of the apparatus.

28. The apparatus of claim 1 wherein:
the apparatus further comprises a storage device; and
the reorderer reorders blocks of the original content item by directly manipulating physical addresses at which the blocks are stored to the storage device.

29. An apparatus comprising:
storage for a local key;
storage for a block reordering structure;
a reorder structure generator for generating the block reordering structure according to the local key; and
a content retriever for retrieving blocks of a content item in an original order according to the block reordering structure.

30. The apparatus of claim 29 further comprising:
a storage device for receiving and storing a reordered content item from an external source.

31. The apparatus of claim 30 wherein the content retriever is adapted for retrieving the blocks in only sequential, linear order.

32. The apparatus of claim 30 wherein the content retriever is adapted for retrieving the blocks in random order.

33. The apparatus of claim 30 wherein the storage for the block reordering structure is a protected memory.

34. The apparatus of claim 33 wherein the protected memory is logically protected by an operating system of the apparatus.

35. The apparatus of claim 34 wherein the protected memory is physically protected against tampering.

36. The apparatus of claim 33 wherein the protected memory comprises means for preventing physical access to electrical signals and devices in the protected memory.

37. The apparatus of claim 30 wherein the block reordering structure comprises:
a plurality of entries, each entry correlating, for a respective original content block, a sequential order placement of that block in the content item with a sequential order placement of that block in a block-reordered version of the content item.

38. The apparatus of claim 37 wherein the plurality of entries comprises a linked list.

39. The apparatus of claim 37 wherein the plurality of entries comprises a table.

40. The apparatus of claim 30 wherein the reorder structure represents a logical addressing reordering of the blocks.

41. The apparatus of claim 30 wherein the reorder structure represents a physical addressing reordering of the blocks.

42. The apparatus of claim 30 further comprising means for receiving the content item in a reordered order from a distribution channel.

43. The apparatus of claim 42 wherein the distribution channel comprises a wireless broadcast channel.

44. The apparatus of claim 42 wherein the distribution channel comprises a coaxial cable.

45. The apparatus of claim 42 wherein the distribution channel comprises a digital subscriber line.

46. The apparatus of claim 42 wherein the distribution channel comprises a removable disk drive.

47. The apparatus of claim 30 wherein the reordered blocks retrieved by the content retriever are unencrypted copies of blocks of an original content item.

48. The apparatus of claim 30 wherein the blocks include a first block and a second block of a same block size.

49. The apparatus of claim 30 wherein the blocks include a first block and a second block of different block sizes.

50. The apparatus of claim 30 wherein the reordered content item comprises an electronic programming guide.

51. The apparatus of claim 30 wherein the reordered content item comprises ATVEF information.

52. The apparatus of claim 30 wherein the reordered content item comprises a digital gift certificate.

53. The apparatus of claim 30 wherein the reordered content item comprises an electronic coupon.

54. The apparatus of claim 30 wherein the reordered content item comprises a movie.

55. The apparatus of claim 30 wherein the reordered content item comprises an episode of a television show.

56. An apparatus comprising:

a server including,

a stored copy of a client identifier;

a key generator for generating a reordering key according to the copy of the client identifier, and

means for transmitting a content item to a client in a reordered block format according to the reordering key; and

the client including,

the client identifier,

client storage for storing the reordered block format content item, and

means for accessing the content item from the client storage in an original block order.

57. The apparatus of claim 56 wherein the server and the client are adapted to transfer the reordered block format content item over a wireless broadcast channel.

58. The apparatus of claim 56 wherein the server and the client are adapted to transfer the reordered block format content item over a coaxial television cable.

59. The apparatus of claim 56 wherein the server and the client are adapted to transfer the reordered block format content item over a digital subscriber line.

60. The apparatus of claim 56 wherein corresponding respective blocks of the content item in its original block order and reordered block format contain substantially identical data values.

61. The apparatus of claim 56 wherein the content item comprises a plurality of blocks, each of a same block size.

62. The apparatus of claim 56 wherein the content item comprises a plurality of blocks of variable block size.

63. The apparatus of claim 56 wherein:

the apparatus further comprises a plurality of such clients;

the server maintains a list of respective client identifiers for the plurality of such clients;

the key generator generates a unique key for each such client; and

for each of two or more clients receiving the reordered block format content item, the means for transmitting generates a uniquely reordered block format content item.

64. The apparatus of claim 56 further comprising:
two or more distinct pluralities of such clients;
a plurality of such servers, each in communication with a respective distinct plurality of such clients; and
each respective server's means for transmitting being configured to reorder blocks of the content item in an order which is reorderable only by the plurality of clients with which that respective server is in communication.

65. The apparatus of claim 56 wherein the client identifier is a serial number.

66. The apparatus of claim 56 wherein the client identifier is a random number.

67. The apparatus of claim 66 wherein the random number is likely to be prime.

68. The apparatus of claim 66 wherein the random number is prime.

69. The apparatus of claim 56 further comprising:
a key channel for communicating the key between the client and the server ; and
a content channel for communicating the content between the server and the client.

70. The apparatus of claim 69 wherein the key channel and the content channel are logical channels carried over one physical communication medium.

71. The apparatus of claim 56 wherein the content item comprises an electronic programming guide.

72. The apparatus of claim 56 wherein the content item comprises ATVEF information.

73. The apparatus of claim 56 wherein the content item comprises a digital gift certificate.

74. The apparatus of claim 56 wherein the content item comprises an electronic coupon.

75. The apparatus of claim 56 wherein the content item comprises a movie.

76. The apparatus of claim 56 wherein the content item comprises an episode of a television show.

77. A cable set-top box comprising:

protected memory which is adapted for storing,

a substantially unique identifier value,

a local key, and

a block reordering structure;

a storage device which is adapted for storing a reordered content item;

a reorder structure generator adapted to create the block reordering structure according to the local key; and

a content retriever adapted to fetch blocks of the reordered content item according to the block reordering structure.

78. The cable set-top box of claim 77 wherein:

the reordered content item is a first reordered content item and the storage device is further for storing a second reordered content item;

the first reordered content item comprises an electronic programming guide; and

the second reordered content item is a video content item.

79. A method of transmitting an original content item from a first entity to a second entity which has an identifier value, comprising:

generating a key as a function of the identifier value;

reordering blocks of the original content item as a function of the key, to create a reordered content item;

delivering the reordered content item to the second entity;

creating a block reordering structure within the second entity; and

accessing a block of the original content item by retrieving it from the reordered content item according to the block reordering structure.

80. The method of claim 79 further comprising:

generating a local key within the second entity, in response to which the block reordering structure is created.

81. The method of claim 80 wherein the second entity generates the local key according to the identifier value of the second entity.

82. A method of protecting an original content item which has blocks in an original order, comprising:

reordering blocks of the original content item in a new order which is different than the original order, according to an identifier value of an intended recipient; and

writing the reordered blocks to either storage or a communication channel in the new order.

83. The method of claim 82 wherein the intended recipient comprises a set-top box and the identifier value comprises a serial number of the set-top box.

84. The method of claim 83 further comprising a server maintaining a list of respective serial numbers of a plurality of set-top boxes.

85. The method of claim 84 further comprising the server reordering and writing the blocks in a unique order for each of two or more of the set-top boxes which have unique serial numbers.

86. A method of accessing a content item by an intended recipient having an identifier value, wherein the content item includes a block having an original order position and a new order position which is different than the original order position, the method comprising:

storing an identification of a relationship between the original order position and the new order position of the block; and

accessing the block by using the stored relationship identification to retrieve the block from the new order position in response to a request to retrieve it from the original order position.

87. The method of claim 86 wherein the intended recipient is a set-top box and the method further comprises generating the identification of the relationship according to an identifying value of the set-top box.

88. The method of claim 87 wherein the identifying value comprises a serial number.

89. The method of claim 87 wherein the identifying value comprises a random number.

90. The method of claim 87 wherein the identifying value comprises a session key.

91. A recordable medium having recorded thereon a reordered content item resulting from the process comprising:

generating a key in response to an identifier value of a content retrieval entity; and

reordering, as controlled by the key, blocks of an original content item to create the reordered content item.

92. The recordable medium of claim 91 wherein the reordered content item results from the process further comprising:

the process being performed in a server, and the content retrieval entity being one of a plurality of clients connectable to the server; and

the server maintaining a list of respective identifier values of the clients.

93. The recordable medium of claim 92 wherein the reordered content item results from the process further comprising:

the server creating the respective identifier values of the clients to be mutually unique.

94. The recordable medium of claim 93 wherein the reordered content item results from the process further comprising:

the server creating the respective identifier values of the clients as serial numbers.

95. The recordable medium of claim 93 wherein the reordered content item results from the process further comprising:

the server creating the respective identifier values of the clients as random numbers.

96. The recordable medium of claim 95 wherein the reordered content item results from the process further comprising:

the server checking the random numbers for at least a threshold likelihood of primeness.

Abstract of the Disclosure

An apparatus and method for protecting a content item such as a digitally encoded movie, an electronic programming guide, or the like, by reordering blocks of the content item prior to transmitting it to a receiving device. The receiving device constructs a block reordering structure which is used to access the reordered content item, to facilitate retrieval of a desired block from the original content item. The reordering may be done responsive to an identifier value of the receiving device, such as a serial number.

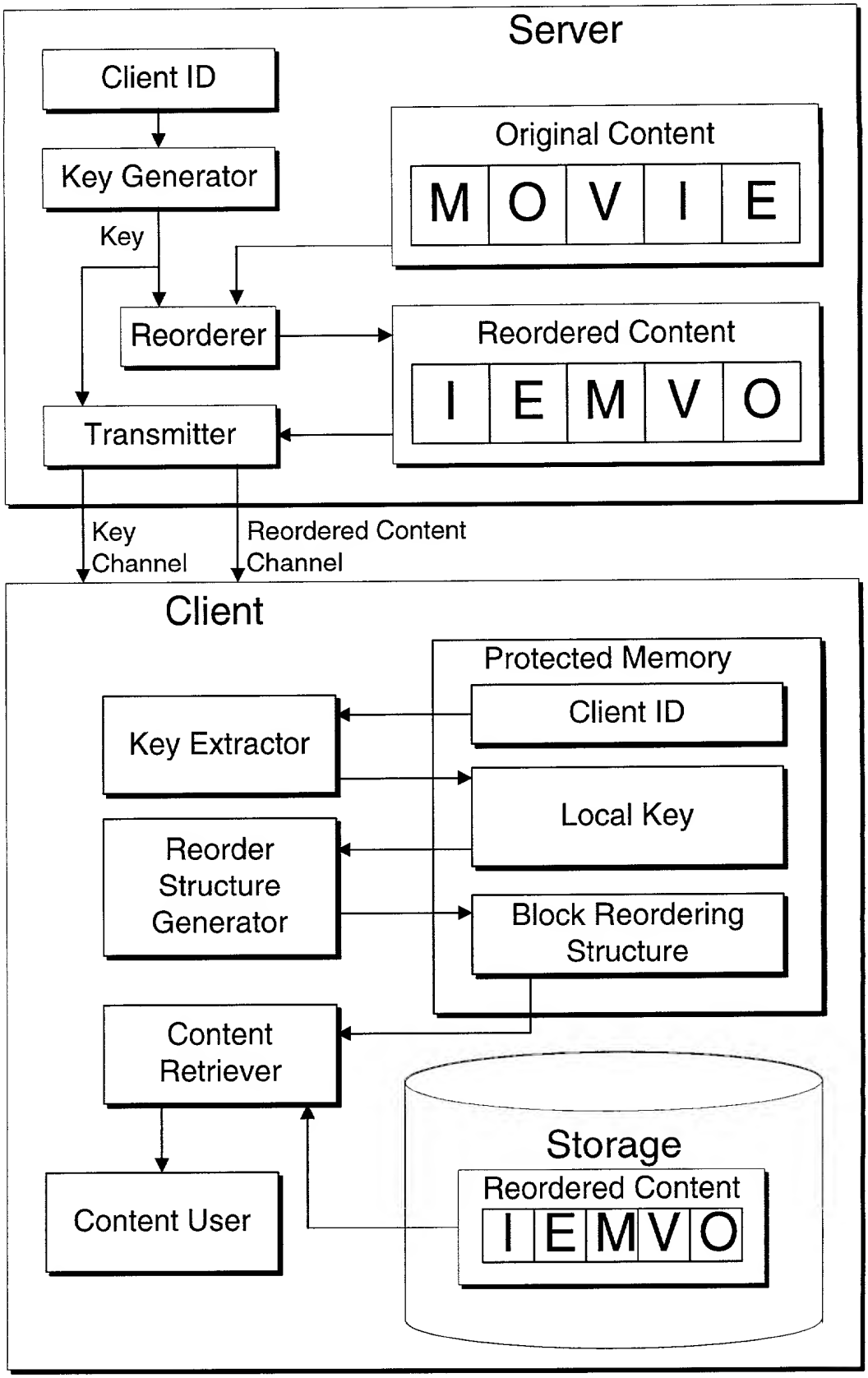

Server
Client ID
Key Generator
Key
Original Content
M O V I E
Reorderer
Reordered Content
I E M V O
Transmitter
Key Channel
Reordered Content Channel
Client
Protected Memory
Client ID
Key Extractor
Local Key
Reorder Structure Generator
Block Reordering Structure
Content Retriever
Storage
Reordered Content
I E M V O
Content User

Fig. 1

50

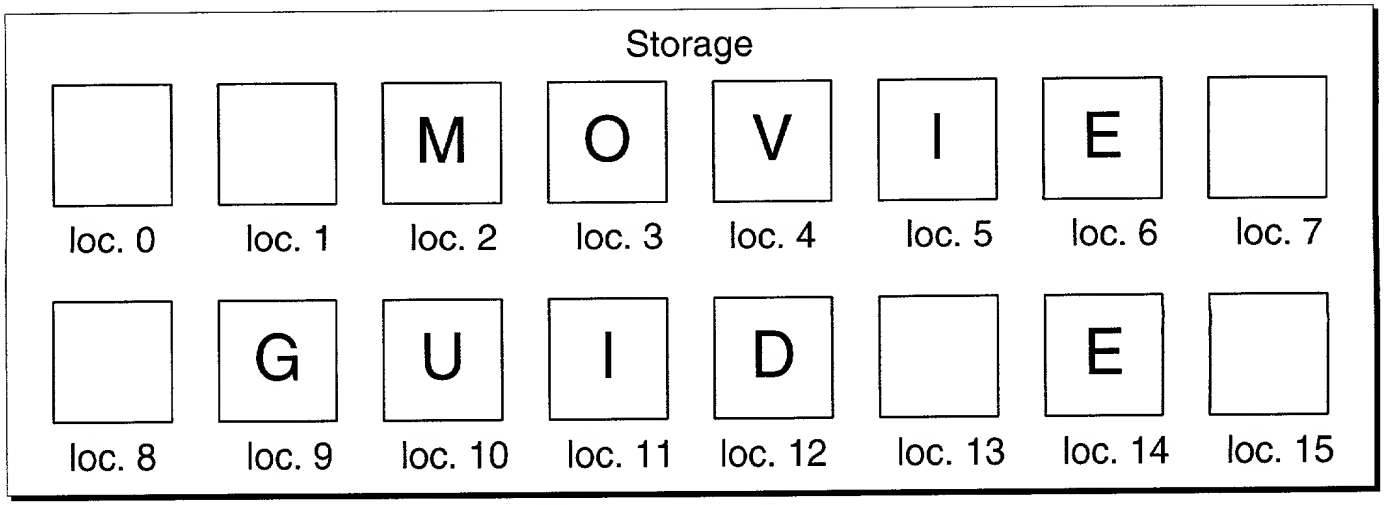


Fig. 2A - prior art

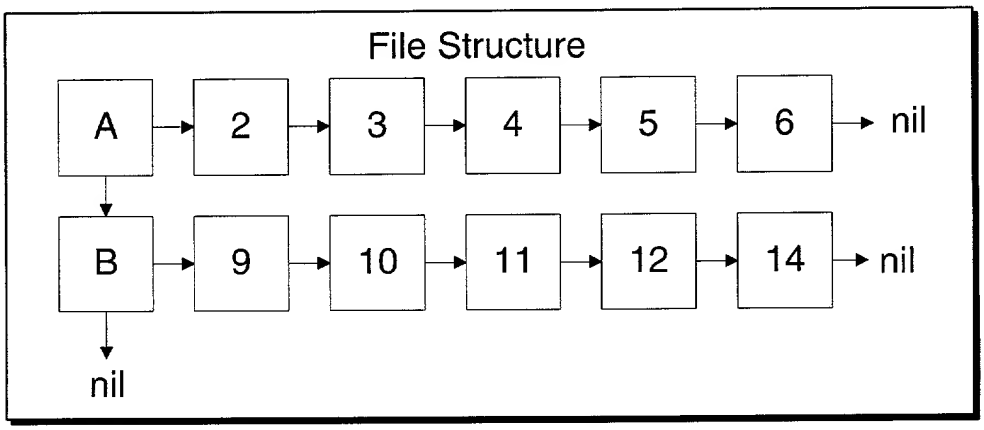


Fig. 2B - prior art

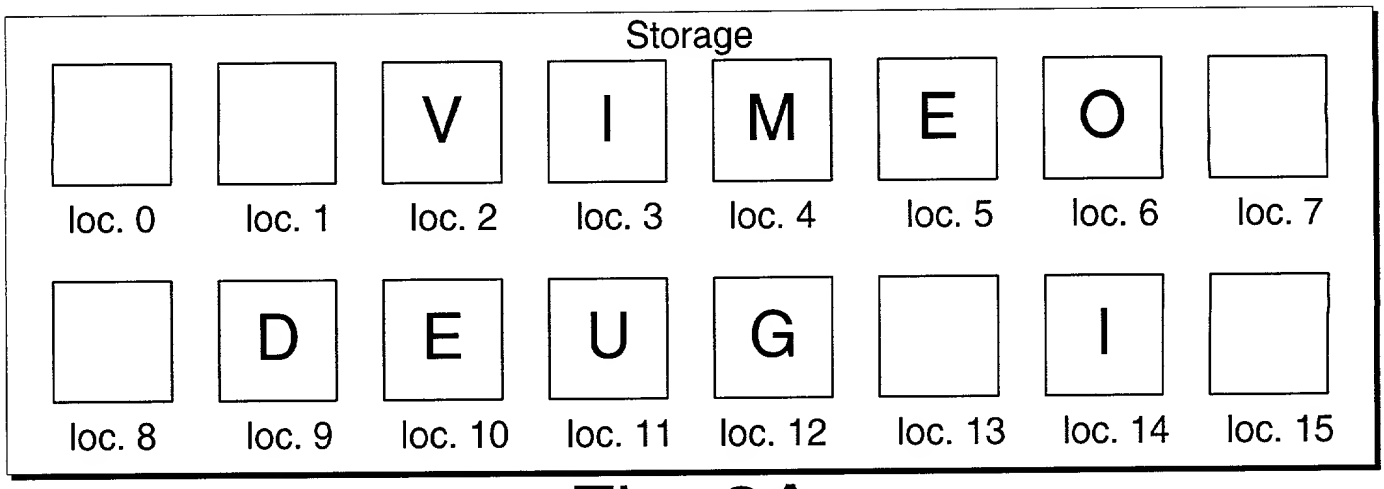
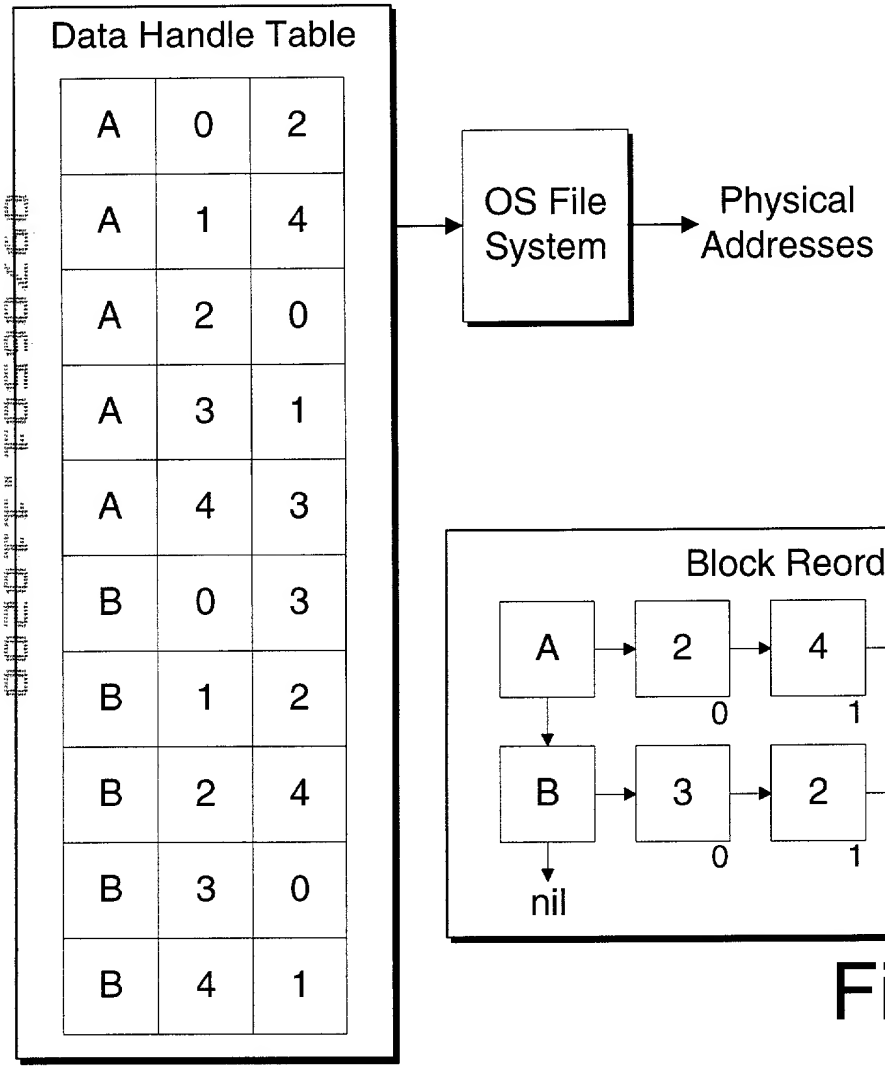


Fig. 3A



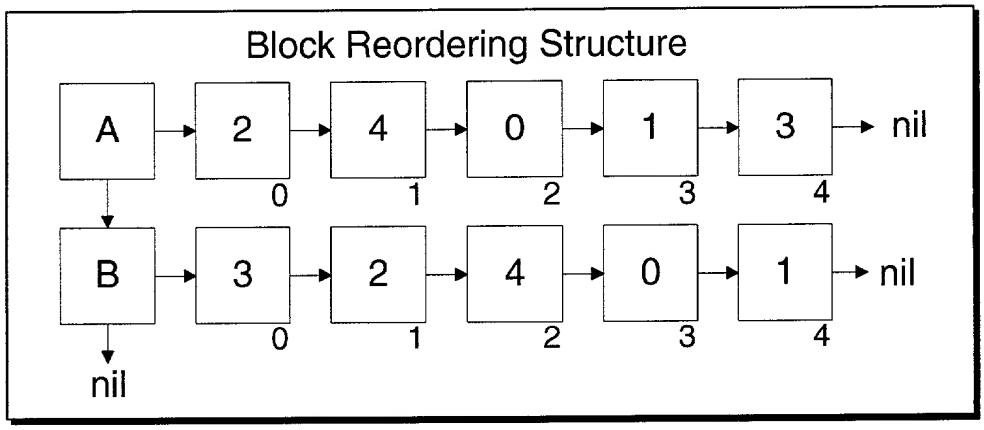


Fig. 3B

Fig. 3C

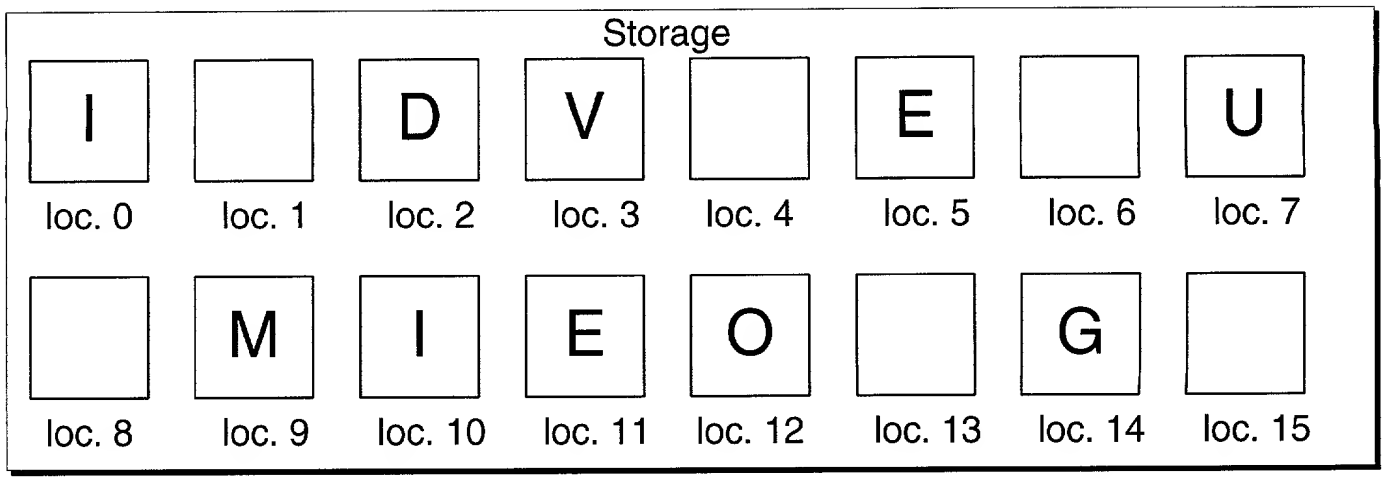


Fig. 4A

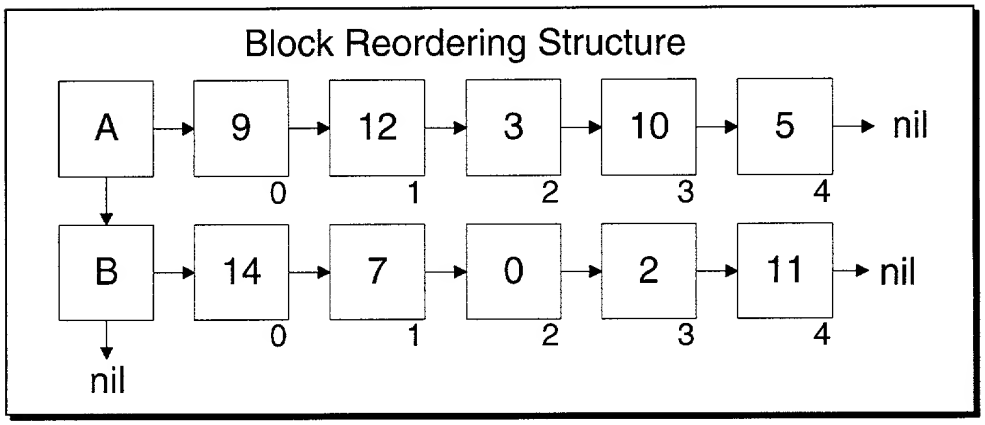


Fig. 4B

Data Handle Table

A	0	9
A	1	12
A	2	3
A	3	10
A	4	5
B	0	14
B	1	7
B	2	0
B	3	2
B	4	11

Fig. 4C

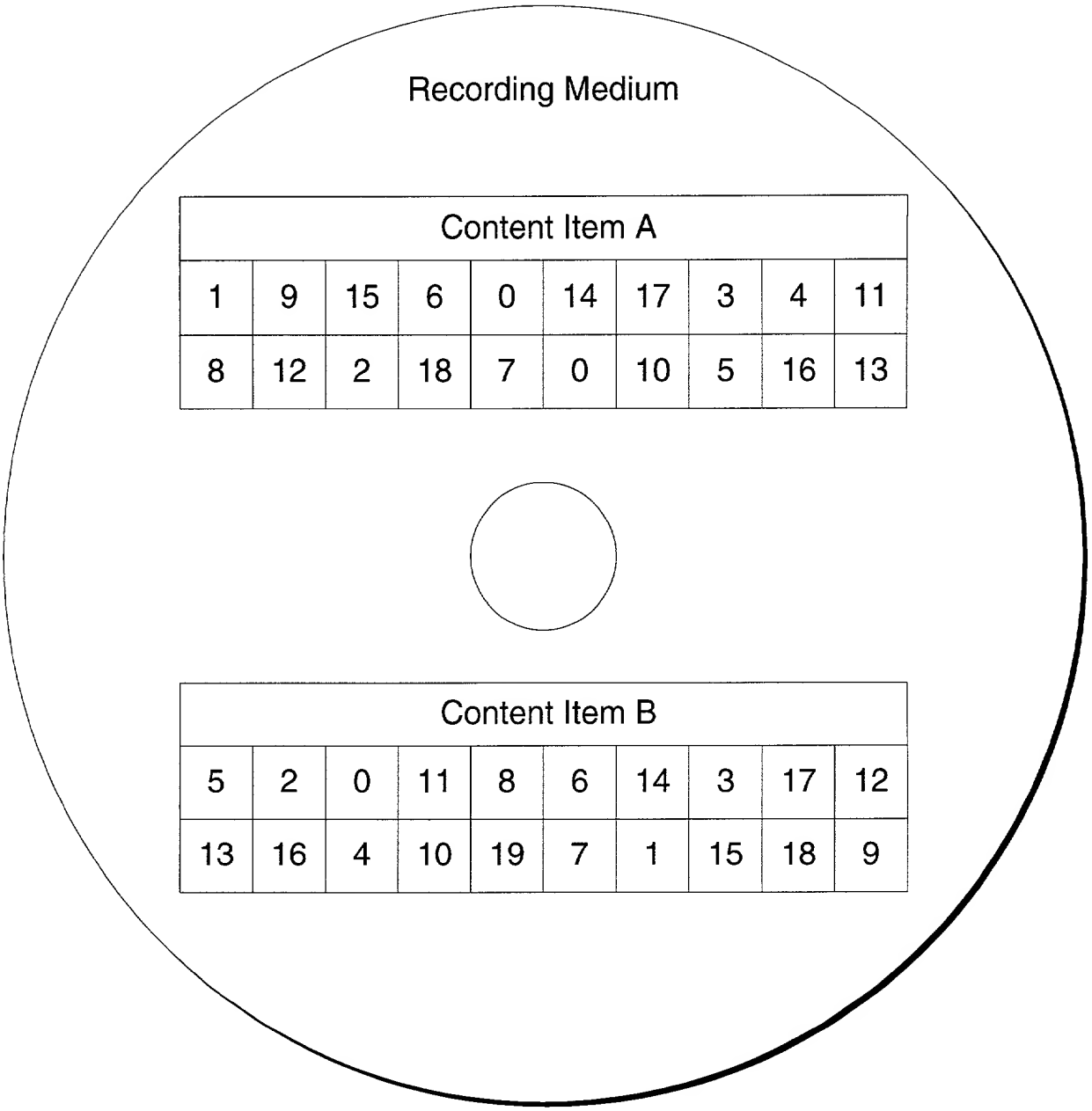


Fig. 5

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

CONTENT PROTECTION USING BLOCK REORDERING

the specification of which

[X] is attached hereto.
[ ] was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, **month**, year)	PRIORITY CLAIMED UNDER 37 USC 119
			☐ No ☐ Yes
			☐ No ☐ Yes
			☐ No ☐ Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:
Richard C. Calderwood, Reg. No. 35,468, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
(Name of Attorney or Agent)
12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:
Richard C. Calderwood, (503) 684-6200.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (given name, family name) **Oleg Rashkovskiy**

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) *(Country)*

P. O. Address _____

_____

Full Name of Second/Joint Inventor (given name, family name) **Eric C. Hannah**

Inventor's Signature _____ Date _____

Residence Pebble Beach, California USA (City, State) Citizenship USA (Country)

P. O. Address 3046 Strawberry Hill

Pebble Beach, California 93953 USA

Full Name of Third/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

_____

Full Name of Fourth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

_____

Full Name of Fifth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

P. O. Address _____

_____

Full Name of Sixth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

Full Name of Seventh/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

Full Name of Eighth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

Full Name of Ninth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

Full Name of Tenth/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

Full Name of Eleventh/Joint Inventor (given name, family name) _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Florin Corie, Reg. No. 46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, Reg. No. P46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 37,374; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; George B. Leavell, Reg. No. 45,436; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Kurt P. Leyendecker, Reg. No. 42,799; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Gregg A. Peacock, Reg. No. 45,001; Marina Portnova, Reg. No. P45,750; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Thomas A. Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Justin M. Dillon, Reg. No. 42,486 and Raul Martinez, Reg. No. 46,904, my patent agents; of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; Steven D. Yates, Reg. No. 42,242, and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. 44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.